

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
CELLULAR DEVICE ASSIGNED CALL
NUMBER 816-894-9594 THAT IS STORED
AT PREMISES CONTROLLED BY AT&T
CORP.

Case No. 22-SW-03054-WJE

FILED UNDER SEAL

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Special Agent Isaac A.W. McPheeters, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for information associated with a certain cellular device assigned with call number 816-894-9594 (the “TARGET TELEPHONE”), with listed subscriber “J.O.”, that is in the custody or control of **AT&T Corp.**, a wireless communications service provider that is headquartered in North Palm Beach, Florida, a location within the Southern District of Florida. As a provider of wireless communications service, **AT&T Corp.** is a provider of an electronic communications service, as defined in 18 U.S.C. § 2510(15).

2. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) and Federal Rule of Criminal Procedure 41 to require **AT&T Corp.** to disclose to the government the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

3. Because this warrant seeks the prospective collection of information, including

cell-site location information, that may fall within the statutory definitions of information collected by a “pen register” and/or “trap and trace device,” *see* 18 U.S.C. § 3127(3) & (4), the requested warrant is designed to also comply with the Pen Register Act. *See* 18 U.S.C. §§ 3121-3127. The requested warrant therefore includes all the information required to be included in an order pursuant to that statute. *See* 18 U.S.C. § 3123(b)(1).

4. I am a Special Agent with the Federal Bureau of Investigation (“FBI”), and I have been employed with the FBI since January 2017. I am currently assigned to the FBI’s Kansas City Field Office of the FBI’s Kansas City Division/Springfield Resident Agency, within the Western District of Missouri. My duties include the investigation of possible violations of federal terrorism offenses, both international and domestic, threats, bombings, and other terrorism offenses. My investigations have included the use of various surveillance techniques and the application for and execution of various search, seizure, and arrest warrants, including search warrants for electronic information.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 371 (“Conspiracy to commit offense or to defraud United States”) are being committed by “B.P.”, “J.O.”, and/or other known or unknown individuals in that they have conspired to violate Title 18, United States Code, Section 249(a)(1), (“Offenses involving actual or perceived race, color, religion, or national origin”) as well as Title 18, United States Code, Section 875(c) (“Communicating an interstate threat”). There is also

probable cause to search the information described in Attachment A for evidence, instrumentalities, and contraband of these crimes as further described in Attachment B.

7. The Court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

8. In September 2022, the Federal Bureau of Investigation (“FBI”) received an anonymous tip via the FBI’s National Threat Operations Center that the user of TikTok account @trashpanda1774 posted a video about conducting a violent attack against the United States (“U.S.”) Government, and starting a war against the government, specifically saying, “I am probably the only one right now that is ready to go to war against this government and I don’t mean just talk about it I mean grab my rifle and go to DC and take this country back physically, not sit in a basement and talk about it.” In addition, the complainant referenced having observed posts in which the user stated the need for six (6) like-minded individuals with firearms and their own gear to conduct a hit. This tip related to an investigation by the FBI’s Memphis division on “B.P.”

9. The FBI conducted subsequent investigative review of TikTok account @trashpanda1774. Upon doing so, other similar videos were observed posted to the account. In one video, dated September 12, 2022, the user can be heard in the video referencing that members of the U.S. Border Patrol were allowing illegal immigrants into the U.S. from Mexico. The user goes on to state that this action was an act of treason and that the U.S. Constitution says the penalty for treason is death. Later in the same video, the user states that he created his TikTok account not

to gain followers but to recruit members into his group, which he refers to as the Second American Militia, and that they “are getting ready to move out”.

10. In another video posted to the TikTok account @trashpanda1774, posted on September 16, 2022, the user references being ready to take back the country very soon. The user further states his intention to “take this country back,” saying, “When we do, we will eradicate every motherfucker that is part of a communist mindset. You can take that to the fucking bank. No mercy. No surrender.”

11. In another video posted to the TikTok account @trashpanda1774, posted on September 20, 2022, the user states that he does not support any type of government and does not support law enforcement. The user also states that “a war is coming.” This video was recorded by an individual with a male voice who appears to be on the front porch of a residence or other structure.

12. In yet another video posted to the TikTok account @trashpanda1774, posted on September 22, 2022, the user states that his group is “moving out as soon as possible” and “we’re out to shoot to kill. We’re not out to maim people or let them go”. In follow-up comments made by the user of @trashpanda1774 following the video, the user posted a comment saying, “where we plan on going when the gun fight starts its going to be hard as shit for other groups to come join”.

13. On September 15, 2022, an emergency disclosure request was issued to TikTok by the FBI regarding username @trashpanda1774. In response, TikTok provided subscriber information for the account, including the email address trashpanda1776@yahoo.com.

14. On September 15, 2022, an emergency disclosure request was issued to Yahoo by the FBI for the email address trashpanda1776@yahoo.com. In response, Yahoo provided

subscriber information for the email address, including the telephone number 931-401-7717 (“7717”).

15. The FBI conducted database checks for the phone 7717. The results of these checks identified “B.P.”, who had a residential address of 974 Swift Drive, Clarksville, Tennessee 37040. Subsequent database checks further revealed that **AT&T Corp.** was the service provider for 7717.

16. On September 23, 2022, the FBI obtained and served a subpoena to **AT&T Corp.** for subscriber information and toll records related to the number 7717. In response, **AT&T Corp.** listed the subscriber of the account as being “B.P.”, with a residential address of 974 Swift Drive, Clarksville, Tennessee 37040. Additionally, the records indicated the account was presently in ‘Active’ status and had been so since approximately October 2018.

17. Based on the aforementioned information, the FBI was able to confirm that “B.P.” is the subscriber to the TikTok account with username @trashpanda1774.

IDENTIFICATION OF TARGET TELEPHONE

18. The FBI conducted a review of the toll records for the 7717 number in order to identify the most commonly connected numbers. As of August 2022, one of those telephone numbers was 816-894-9594 (TARGET TELEPHONE).

19. The FBI conducted database checks to identify the account holder for the TARGET TELEPHONE. The results of these checks indicated that the account belonged to two individuals, one of whom named “J.O.” and a likely relative of “J.O.” Subscriber records indicated that the TARGET TELEPHONE was owned by “J.O.”’s relative.

20. A driver’s license check of the Missouri Department of Motor Vehicles database associated “J.O.” with a residential address of 34154 Highway 65, Warsaw, Missouri 65355, a location within the Western District of Missouri.

21. As mentioned in Paragraph 11 above, “B.P.” recorded and posted a TikTok video while on the front porch of a structure. The FBI conducted a Google Maps search for the address associated with “J.O.” and also conducted physical surveillance on the residence. The FBI found that the exterior of the home located at the address was consistent with what could be seen in the TikTok video based on commonalities between the Google Maps image and the video, including the structure of the front porch, the presence of an American flag and its location on the front of the residence, and similar vegetation in and around the property. Based on this, the FBI concluded that “B.P.” was co-located at “J.O.”’s residence as of September 20, 2022.

22. On September 25, 2022, a video was posted to the TikTok account @mobornfromthe90s showing “J.O.” speaking to the camera, expressing a desire to secure the southern border. The TikTok account appeared to be used by “J.O.” In comments on the video, “J.O.” indicates they are leaving for Texas on October 4, 2022.

23. On September 28, 2022, the FBI reviewed the TikTok account with username @trashpanda1774, subscribed to by “B.P.”, and found that the language on the homepage for the account had been updated to say, “MO is now home”. Based on your Affiant’s knowledge and experience, MO is the two-letter abbreviation for Missouri, which leads to the conclusion that “B.P.” remains in Missouri.

24. On September 29, 2022, physical surveillance conducted by the FBI at 34154 Highway 65, Warsaw, Missouri, observed a white Ford F250 pickup at the residence. Based upon information received from the Missouri Department of Revenue, “J.O.” has a 2015 Ford F250 registered in his name. Physical surveillance that same day observed a silver Jeep Grand Cherokee registered to “B.P.” parked at the residence.

25. On September 30, 2022, physical surveillance conducted by the FBI at 34154

Highway 65, Warsaw, Missouri, again observed the Jeep registered to “B.P.” parked at the residence. That same day, “B.P.” was observed walking into and out of a UMB Bank, 707 Walnut Drive, Warsaw, Missouri. “B.P.” was then observed walking into and out of Top Gun Armory, 619 Commercial St, Warsaw, Missouri. “B.P.” was observed open carrying what appeared to be a handgun on his hip in a holster. Law enforcement records indicate “B.P.” is a convicted felon and is prohibited from possessing firearms.

26. On October 2, 2022, an FBI Undercover Employee (“UCE”) called “J.O.” at the TARGET TELEPHONE number. During that phone call, “J.O.” said he wanted to get a group together to secure the border between the United States and Mexico. “J.O.” asked the UCE if the UCE could acquire HAM radios for “J.O.” with encrypted channels. “J.O.” indicated he could trade firearm parts and ammunition for the HAM radios. “J.O.” asked the UCE if the UCE could acquire “NVGs.” I know from my training and experience that “NVGs” is a common acronym for night vision goggles which are commonly used by highly trained military and law enforcement units to allow them to operate in darkness. “J.O.” told the UCE that it did not matter if someone was a felon; they should not lose their right to firearms. “J.O.” told the UCE that he was already practically a terrorist. “J.O.” told the UCE, “We’re on the verge of fuckin’ waivin’ the red flag, and what I mean by that is like no prisoners.” “J.O.” further told the UCE, “If someone pops over the border, they’re getting dropped right then and there. I know that sounds cruel and inhumane, but what people don’t understand is that we consistently turn into this we’re gonna start having bombings like over in Europe and England.” “J.O.” told the UCE that he had a group of four people and was planning to relocate to Texas on October 4, 2022, or possibly the weekend of October 8, 2022. “J.O.” hoped to start with surveillance and reconnaissance at the border and grow his group over time. “J.O.” said he had already notified the office of the governor of Texas that he was

coming. “J.O.” told the UCE he could die tomorrow, but he would rather die tomorrow knowing he did something.

27. On or around October 2, 2022, “B.P.” posted to his TikTok account, @trashpanda1774, saying “patriots this saturday 10/08/2022 we are going hunting! IYKYK!! Leaving from warsaw, MO 1200 CT.... starting from country mart across from dollar genera. hope to see you there and ready. IYKYK”

28. In my training and experience, I have learned that **AT&T Corp.** is a company that provides cellular communications service to the general public. I also know that providers of cellular communications service have technical capabilities that allow them to collect and generate information about the locations of the cellular devices to which they provide service, including E-911 Phase II data, also known as GPS data or latitude-longitude data and cell-site data, also known as “tower/face information” or cell tower/sector records. E-911 Phase II data provides relatively precise location information about the cellular device itself, either via GPS tracking technology built into the phone or by triangulating on the device’s signal using data from several of the provider’s cell towers. Cell-site data identifies the “cell towers” (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular device and, in some cases, the “sector” (i.e., faces of the towers) to which the device connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate general location of the cellular device and is typically less precise than E-911 Phase II data.

29. Based on my training and experience, I know that **AT&T Corp.** can collect E-911 Phase II data about the location of the TARGET TELEPHONE, including by initiating a signal to

determine the location of the TARGET TELEPHONE on **AT&T Corp.**'s network or with such other reference points as may be reasonably available.

30. Based on my training and experience, I know that **AT&T Corp.** can collect cell-site data on a prospective and historical basis about the TARGET TELEPHONE. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as **AT&T Corp.** typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

31. Based on my training and experience, I know that the telephone service providers can collect per-call measurement data, which each provider may refer to with a specific name. Verizon refers to this data as Real-Time Tool ("RTT"). T-Mobile refers to the data as timing advance. AT&T refers to the data as NELOS. Sprint refers to the data as per call measurement data ("PCMD"). The per-call measurement data estimates the approximate distance of the cellular device from a cellular tower based upon the speed with which signals travel between the device and the tower. This information can be used to estimate an approximate location range that is more precise than typical cell site data.

32. Based on my training and experience, I know each cellular device has one or more unique identifiers embedded inside it. Depending on the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an

Electronic Serial Number (“ESN”), a Mobile Electronic Identity Number (“MEIN”), a Mobile Identification Number (“MIN”), a Subscriber Identity Module (“SIM”), a Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), an International Mobile Subscriber Identifier (“IMSI”), or an International Mobile Equipment Identity (“IMEI”). The unique identifiers – as transmitted from a cellular device to a cellular antenna or tower – can be recorded by pen-trap devices and indicate the identity of the cellular device making the communication without revealing the communication’s content.

33. Based on my training and experience, I know that wireless providers such as **AT&T Corp.** typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless communication service. I also know that wireless providers such as **AT&T Corp.** typically collect and retain information about their subscribers’ use of the wireless service, such as records about calls or other communications sent or received by a particular device and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the TARGET TELEPHONE’s user or users and may assist in the identification of co-conspirators and/or victims.

34. Records of customer and subscriber information relating to this investigation that are available from **AT&T Corp.**, and the contents of electronic communications that may be found at **AT&T Corp.**, will help government investigators to identify the individual(s) who are responsible for the events described above and to determine the nature and scope of their activities. Accordingly, the government requests that **AT&T Corp.** be directed to produce all records

described in Attachments A and B to the proposed Search Warrant.

35. Part C of Attachment B requests the contents of all electronic communications located in **AT&T Corp.**'s computer systems in directories or files owned or controlled by the accounts identified in Attachment A. These stored files, covered by 18 U.S.C. § 2703(a), will help ascertain the scope and nature of the activity conducted by the subscriber, owner, and/or controller of the directories or files.

AUTHORIZATION REQUEST

36. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c). The proposed warrant will also function as a pen register order under 18 U.S.C. § 3123 authorizing the installation and use of a pen register and/or trap and trace device to record, decode, and/or capture certain information in Attachment A for each communication to or from the TARGET TELEPHONE, without geographic limit, for a period of 45 days pursuant to 18 U.S.C. § 3123(c)(1).

37. I further request that the Court direct **AT&T Corp.** to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on **AT&T Corp.**, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

38. I further request that the Court direct **AT&T Corp.** to disclose to the government any information described in Attachment B that is within the possession, custody, or control of **AT&T Corp.** I also request that the Court direct **AT&T Corp.** to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with

AT&T Corp.'s services, including by initiating a signal to determine the location of the Target Cell Phone on AT&T Corp.'s network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate AT&T Corp. for reasonable expenses incurred in furnishing such facilities or assistance.

39. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,



Isaac A.W. McPheeters
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me by telephone or other reliable electronic means on the 3rd day of October 2022.



Willie J. Epps, Jr.
United States Magistrate Judge